

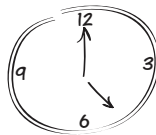
Registering your FortiGate and configuring the system settings

In this example, you will register your FortiGate unit and set the system time. You will also configure several administrative account settings to prevent unauthorized access.

1. Registering your FortiGate
2. Setting the system time
3. (Optional) Restricting administrative access to a trusted host
4. Changing the default admin password
5. Results



*Register your
FortiGate*



*Set the
system time*



*Configure the
admin account*

1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to support.fortinet.com.

Before registering your FortiGate unit, it must have Internet connectivity.

Go to **System > Dashboard > Status** and locate the **License Information** widget.

Next to **Support Contract**, select **Register**.



Either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.

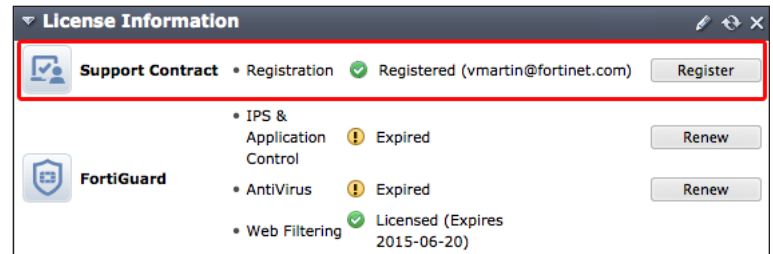


It is recommend to use a common account to register all your Fortinet products, to allow the Support site to keep a complete listing of your devices.

Register this FortiGate with FortiCare by logging in or creating a new account

Serial Number	FG100D3G12812324
Action	<input checked="" type="radio"/> Login <input type="radio"/> Create Account
Email	<input type="text" value="vmartin@fortinet.com"/>
Password	<input type="password" value="....."/>
Country	<input type="text" value="Canada"/>
Reseller	<input type="text" value="Other"/>

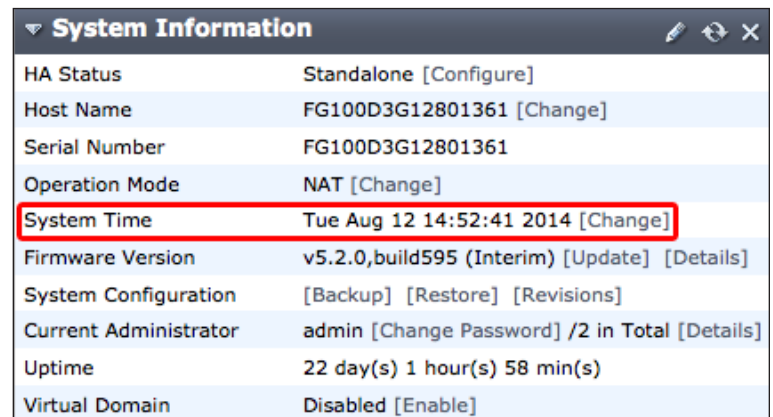
The **License Information** widget now displays the unit as **Registered**.



2. Setting the system time

Go to **System > Dashboard > Status** and locate the **System Information** widget.

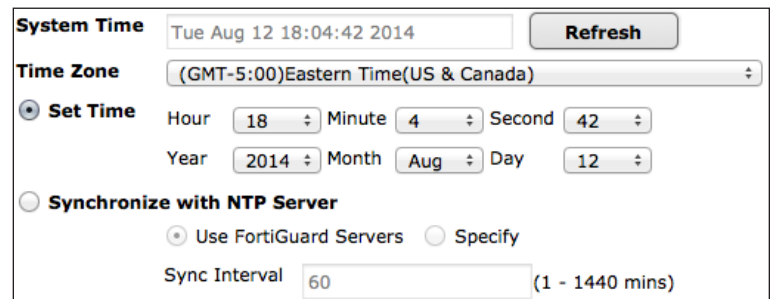
Next to **System Time**, select **Change**.



Select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.



Since not all time zones have names, you may need to know how many hours ahead (+) or behind (-) you are from Greenwich Mean Time (GMT).



The **System Information** widget now displays the correct time.

System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12801361 [Change]
Serial Number	FG100D3G12801361
Operation Mode	NAT [Change]
System Time	Tue Aug 12 18:04:49 2014 [Change]
Firmware Version	v5.2.0,build595 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]
Uptime	22 day(s) 1 hour(s) 58 min(s)
Virtual Domain	Disabled [Enable]

3. (Optional) Restricting administrative access to a trusted host



Go to **System > Admin > Administrators** and edit the default *admin* account.

Enable **Restrict this Administrator Login from Trusted Hosts Only**. Set **Trusted Host #1** to the static IP address of the PC you will use to administer the FortiGate unit, using /32 as the netmask.

You can also set an entire subnet as the trusted host, using /24 as the netmask.

If required, set additional trusted hosts.

☒ Restrict this Administrator Login from Trusted Hosts Only

Trusted Host #1	192.168.220.110/32
Trusted Host #2	0.0.0.0/0.0.0.0
Trusted Host #3	0.0.0.0/0.0.0.0 
IPv6 Trusted Host #1	::/0
IPv6 Trusted Host #2	::/0
IPv6 Trusted Host #3	::/0 

4. Changing the default admin password

Go to **System > Admin > Administrators** and edit the default *admin* account.

Select **Change Password**. Leave **Old Password** blank and enter the **New Password**.

You will be automatically signed out after changing the password.

Administrator	admin
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

5. Results

Attempt to log in using the *admin* account without a password. Access is denied.

Log in using the new password to access the FortiGate.

Authentication failure. Please try again...

Name	<input type="password"/>
Password	<input type="password"/>

Login

Go to **System > Dashboard > Status** and locate the **Alert Message Console** widget, which indicates the failed authentication attempt.

(Optional) If access has been restricted to a trusted host, attempts to connect from a device that is not trusted will be denied.

Alert Message Console

2014-08-12 12:41:13 Failed authentication attempt for admin